SYSTEM AND PROTOCOL FOR FRAME RELAY SERVICE OVER THE INTERNET

Related Applications

This application is a continuation of U.S. Serial No. 09/871,165, filed on May 31, 2001, which is a continuation of U.S. Serial No. 09/663,486, filed on September 13, 2000.

Field of the Invention

The present invention relates generally communications, and more particularly to a system and protocol for frame relay communications over the Internet.

Background Information

Frame Relay is an access standard defined by the ITU-T in the I.122 recommendation, "Framework for Providing Additional Packet Mode Bearer Services." Frame Relay services employ a form of packet switching analogous to a streamlined version of X.25 networks. The packets are in the form of "frames" which can be variable in length. Thus a key advantage is that a frame relay network can accommodate data packets of various sizes and that are associated with virtually any native data protocol. Accordingly, frame relay services have become a popular replacement for dedicated or private leased-line connections between enterprise LANs located at multiple sites.

Today, however, service providers (SPs) and their subscribers have another, more cost effective alternative for connecting different sites securely, the Internet. Enterprise subscribers want to preserve their investments in Frame Relay equipment while extending the reach of their private networks to new locations using a lower cost Internet (IP) solution. They also want to extend secure Internet access to existing locations served by frame relay without the additional expense of adding or replacing customer premises equipment (CPE) or acquiring access lines to these locations. They

want to make the transition in a controlled manner at their own pace to minimize risks and maintain access to the existing frame relay network during the migration.

Additionally, current frame relay networks have some limitations. They have no built in access from the frame relay network or cloud to the Internet. Typically, separate arrangements are made for Internet access. Current frame relay networks also lack the Internet security protocol (IPSec) encryption and firewall features required for secure Internet access from corporations. Further, typical service level agreements (SLAs) for frame relay service as defined by the Frame Relay Forum (FRF) are fairly basic and conservative with little opportunity for provider or service differentiation. In contrast, differentiated services allows IP networks to offer enhanced services over and beyond what is currently being standardized by the FRF for frame relay service.

Accordingly, for all the reasons discussed above, and for other reasons that will become apparent upon reading and understanding the present specification, there is a need for a system and protocol that permits frame relay service over the Internet that is secure and provides the flexibility, economy and features provided by the Internet.

Summary of the Invention

In accordance with the present invention, a system for communications over the Internet includes at least one router connectable to a first user or subscriber location. An Internet protocol service processing switch (IPSX) is connected to the at least one router to format or encapsulate the message for secure transmission over the Internet. The message is then preferably transmitted over the Internet via an Internet Protocol Security (IPSec) tunnel for secure transmission to the addressed destination.

In accordance with another embodiment of the present invention, a method for communication over the Internet includes generating a frame relay message. Overhead information may be stripped from the frame relay message and valid frames encapsulated in a frame relay over Internet protocol (FOIP) header. The FOIP header and message payload are encapsulated in a user datagram protocol (UDP/IP) and then

the UDP/IP encapsulated message is transmitted over the Internet to a predetermined destination preferably via an IPSec tunnel.

Brief Description of the Drawings

Figure 1 is a block schematic diagram of a system for communications over the Internet in accordance with one embodiment of the present invention.

Figure 2 is a block schematic diagram of a system for communications over the Internet in accordance with another embodiment of the present invention.

Figure 3 is a block schematic diagram of a system for communications over the Internet for dial-up user access in accordance with a further embodiment of the present invention.

Figure 4 is a block schematic diagram of an IP-enabled frame relay network layered with advanced Internet Application services in accordance with another embodiment of the present invention.

Figure 5 is an illustration of the frame relay frame structure in accordance with one embodiment of the present invention.

Figure 6 is an illustration of the frame relay encapsulation of the IP datagram in accordance with one embodiment of the present invention.

Figure 7 is a flow chart of a method for frame relay communication over the Internet in accordance with one embodiment of the present invention.

Detailed Description of the Embodiments

In the following detailed description of the embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Referring initially to Figure 1, a schematic diagram of a system for communications over the Internet in accordance with at least one embodiment of the

present invention is shown. The system 100 includes a plurality of routers 102 at different locations or sites, Each of the routers 102 is connected to at least one user or subscriber 104. Each router 102 also preferably is associated with at least two data link connection identifiers (DLCIs) 106 for redundancy. The DLCIs 106 are shown in Figure 1 as separate elements but may actually be part of the router 102. The system may also include multiple routers 102 at a site for redundancy.

The router 102/DLCI 106 is connected to an Internet protocol service processing switch (IPSX) 108. The IPSX may be an IPSX 9000™ as manufactured and sold by CoSine Communications, Inc., Redwood City California. In the embodiment shown in Figure 1, the IPSX includes a virtual subscriber switch (VS) 110 coupled at one end to the router 102/DLCI 106 and connected to a virtual router (VR) 112 at another end or terminal. The virtual router (VR) 112 is coupled to a firewall 114 and the firewall 114 is connected to an Internet protocol security (IPSec) module 116. The IPSec 116 is then connectable to the Internet 118 for transmission of frame relay messages to other users/subscribers 104 or locations on the virtual private network (VPN) 120 formed by the system 100. In accordance with the present invention, the connection via the Internet is preferably via an IPSec tunnel 122 to provide secured transmissions from one location or user 104 to another. The connection via the Internet between one location or user 104 and another location or user 104 is analogous to a frame relay permanent virtual circuit (PVC).

The system 100 also includes a transport protocol (TP) for transmitting messages over the Internet. The transport protocol for frame relay payloads is based on user datagram protocol (UDP/IP), which is optionally IPSec ESP (enhanced service provider) protected in the transport mode. IPSec protection may be made the default. The IPSec tunnel 122 uses as the source IP address, the VR's address at the source and the address of the destination VR 112 at the remote end.

The payload transport protocol is complemented by a switch-to-switch signaling protocol (SSFOIP) that operates in parallel. Because multiple virtual switches 110 realizations will exist in distributed fashion, periodic synchronization between the

virtual switches 110 will be necessary. The SSFOIP will also be based on UDP/IP. The SSFOIP is used to communicate status information about the different components within the system and to announce and set up the creation of new components or DLCIs for future service. The SSFOIP protocol header and payload are encapsulated in UDP.

The selection of non-hard state transport protocol such as UDP allows hot standby virtual switches to be easily implemented in the future. This protocol also makes the implementation simpler, more scalable and less susceptible to certain kinds of attacks. Additionally, it allows leverage of any future IP multicast infrastructure that might be deployed.

The virtual switch 110 will also implement the frame relay local management interface (LMI) 124 function for requesting and responding to status inquiry messages from other components in the system 100. For dual homed customer provided equipment (CPE), such as dual routers or dual bridges or other equipment, failure to respond accurately will result in black holed traffic. If a DLCI failure occurs, the system will be able to reroute using an Open System Interconnection (OSI) layer 3 or 2 route calculation algorithm. The SSFOIP is used to communicate status information between the components of the system 100.

The system 100 also includes an operating support system (OSS) 126 connected to the frame relay network 128. The initial provisioning or set up of the private virtual circuits (PVCs) and DLCIs may be done by the OSS 126 and communicated to each IPSX 108 by simple network management protocol (SNMP) which then sets up the VSs 110. A group of VSs that make up the virtual private network (VPN) 120 may then initiate SSFOIP exchanges. The OSS 126 will also be responsible for installing in each VS 110 the information or addresses to reach all other VSs in the VPN 120 or system 100.

Several protocols are currently being transported over frame relay networks that require frame sequence preservation. Two such protocols are system network architecture (SNA) and the IBM NETBIOS. Because normal frame relay service involves explicitly setting up and tearing down PVCs on an end to end basis, sequence

preservation has been straightforward. In the current IP backbone routing environment, however, no such end-to-end mechanism exists. Accordingly, an alternate method of preserving frame sequence is needed.. One approach is to implement an 8-bit sequence number as described in more detail with the in the IP datagram encapsulation of the payload message.

Figure 2 is a block schematic diagram of a system for communications over the Internet in accordance with another embodiment of the present invention. The system 200 of Figure 2 includes a plurality of subscriber remote offices 202. Each of the subscriber remote offices includes a router 204. The subscriber remote office 1 and the subscriber headquarters are each respectively connected to a frame relay network 206. The frame relay network is then connected to an IPSX 208. The IPSX includes a virtual router 210 connected to a firewall 212 and the firewall 212 is also connected to a IPSec module 214 or function. The IPSX 208 may then be connected via an IPSec tunnel 216 to another IPSX 218 through the service providers Internet core 220. In another connection or permanent virtual circuit (PVC), either of the subscriber remote offices 1 or 2 or subscriber headquarters 202 could be interconnected through the Internet to remote office 3 via a router 224 with an IPSec function to provide secure communications over the Internet.

The system 200 of Figure 2 also includes a service management system (SMS) 226 for monitoring and managing traffic flow and to deploy and manage IP features and services to which the user has subscribed. The SMS 226 may be an InVision™ system as provide by CoSine Communications, Inc.

The system 200 of Figure 2 also may include a customer network management (CNM) system 228 to provide reporting, status trend and forecast analysis for network planning and service modification. The CNM 228 may be an InGage™ system as also provided by CoSine Communications.

Figure 3 is a block diagram of a system 300 for communications over the Internet for dial-up user access in accordance with a further embodiment of the present invention. The system 300 is similar to that of Figure 2 except that a dial up user 302

accesses the network or system 300 through the public switched telephone network 304 by dialing a remote access server 306. The dial-up user is then connected to the IPSX 208 through the Internet 222 or the SP IP Core 220.

Figure 4 is a schematic block diagram of an IP-enabled frame relay network 400 layered with advanced Internet application services in accordance with another embodiment of the present invention. The network 400 includes a plurality of different site locations 401-406. Each of the sites 401-406 is connected to an IPSX 408, 410 and 412. Sites 401 and 402 are connected to IPSX 408. Sites 403 and 404 are connected to IPSX 410 and sites 405 and 406 are connected to IPSX 412. The IPSXs 408, 410 and 412 are connected in a daisy chain fashion by a permanent virtual circuit (PVC) 414, 416 and 418. Each of the PVCs may contain a virtual router (not shown in Figure 4). The IPSXs 408 and 412 each include an intrusion detector 420 and 422 to secure access to the Internet 424 and to guard against hackers.

Figure 5 is an illustration a frame relay frame structure 500 in accordance with one embodiment of the present invention. The frame structure 500 includes a high level data link control (HDLC) flag group of bits or field 502, a header field or group of bits 504, an information field 506, a frame check sequence field 508 and another flag field 510. The header field 504 includes a data link connection identifier (DLCI) field or group of bits 512 (high order), a command/response (C/R) field 514, an address extension (E/A) field 516, another low order DLCI field 518, a forward explicit congestion notification (FECN) field (520), a backward explicit congestion notification (BECN) field 522, a discard eligibility (DE) field 524 and another address extension (EA) field 526. The FECN 520 notifies the receiving device that the network is experiencing congestion and the BECN 522 notifies the transmitting device that the network is experiencing congestion. The DE field 524 indicates what may be discarded if the event of network congestion of the subscriber has exceeded his committed burst rate (Bc) or Committed information rate (CIR).

Figure 6 is an illustration of the frame relay encapsulation 600 of the IP datagram for transmission over the Internet by the system 100 or 200. The IP datagram

includes an IP field 602, an enhanced service provider (ESP) field 604 indicating enhanced services, a universal datagram (UDP) field 606, a frame relay over IP (FOIP) field 608 and the FOIP payload field 610. The FOIP field 608 may be further broken down into a control (CTRL) field 612, a connection ID (ConnID) field 614 and flag field 616 and a DLCI field 618. The CTRL field 612 may be further broke down into Vers, Rsvd, Seq for frame sequence order, and Len fields 620-626 as shown in Figure 6. The flag field 616 may also be broken down into Rsvd, FECN, BECN and DE fields 628-634 that have functions similar to that previously discussed. The frame relay payload encapsulation process will be described in more detail with respect to Figure 7.

Figure 7 is a flow chart of the method 700 for frame relay communication over the Internet in accordance with one embodiment of the present invention. In action box 702, a message is created or generated by a user or subscriber 104 in the frame relay protocol or format. The frame check sequence (FCS) is validated in action box 704 and if a frame is found to be valid the HDLC flags and FCS fields are stripped from the message format in action box 706. In action box 708 the valid frames are encapsulated in a FOIP header and in action box 710 the FOIP header and payload are encapsulated in UDP. An assigned number is obtained for the destination UDP port in action box 712 and the message resulting from action box 710 may be further encapsulated in IP with or without IPSec protection in action box 714. Integrity checks may be performed by IPSec where applicable in action box 716 or a UDP checksum may be applied to the message in action box 718 if IPSec is not used. In action box 720 the resulting message is transmitted over the Internet to the destination, preferably via an IPSec tunnel 122.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is intended that this invention be limited only by the claims and the equivalents thereof.